APPLICATION

FOR

UNITED STATES LETTERS PATENT

FOR

# METHOD OF STORING DATA

BY

Alrick Lockhart Smith, Ph.D.

James C. Wray, Reg. No. 22,693
Meera P. Narasimhan, Reg. No. 40,252
1493 Chain Bridge Road
Suite 300
McLean, Virginia 22101
Tel: (703) 442-4800
Fax: (703) 448-7397

# METHOD OF STORING DATA

This application claims the benefit of U.K. Patent Application No. 0215004.3, filed June 28, 2002.

## BACKGROUND OF THE INVENTION

One of the problems with portable computers such as laptops and hand-held computers is that if the computer is lost or stolen it is not possible to recover the data. In addition, there is also the risk that an unauthorized party may access the data.

The aim of the present invention is to address and/or ameliorate some of those risks and problems.

Need exists for more secure methods of storing data.

## SUMMARY OF THE INVENTION

In accordance with a first aspect of the present invention, there is provided a method of storing data for an electronic processing device comprising establishing a data communication link between the electronic processing device and a remote data storage device, transferring the data to the remote data storage device, and deleting the data transmitted to remote data storage device from the electronic processing device.

In accordance with a second aspect of the present invention, there is provided a system for storing data for an electronic processing device, the system comprising a remote data storage device, transmission means to transmit data from the electronic processing device to the remote data storage device, and deletion means to delete the data transmitted to the remote data storage device from the electronic processing device.

The invention has the advantage that by storing data for the electronic processing device on a remote data storage facility, the data can be recovered to another electronic processing device if the electronic processing device is damaged, lost or stolen.

The invention also has the advantage that subsequent deletion of the data from the electronic processing device minimizes the risk of unauthorized access to the data.

Preferably, the system further comprises encryption means to encrypt the data on the electronic processing device, and the data transmitted to the remote data storage device is the encrypted data.

Thus in a related aspect, the present invention provides a method of storing data for an electronic processing device comprising the steps of:

encrypting data in the electronic processing device;

establishing a data communication link between the electronic processing device and a remote data storage device; and

transferring the encrypted data to the remote data storage device.

Typically, any encrypted data also on the electronic processing device is deleted after transfer of the encrypted data to the remote data storage facility.

Preferably, the electronic processing device is a computer and typically, may be a portable computer, such as a laptop, notebook or hand-held computer.

If the electronic processing device is a portable computer, the data communication link that is established may be at least partially a wireless data communication link.

Preferably, the data communication link may be established via a computer network, such as a local area network, a wide area network or the Internet.

These and further and other objects and features of the invention are apparent in the disclosure, which includes the above and ongoing written specification, with the claims and the drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic diagram of a laptop computer coupled to a server on the Internet.

Figure 2 is a flow chart illustrating various steps in a process embodying the present invention.

Figure 3 is a schematic diagram of a laptop coupled to a secure data storage device in different ways.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows an electronic processing device in the form of a laptop computer 1 connected to a wireless communication device.

The wireless communication device 2 may be, for example, in the form of a PCMCIA card incorporating a mobile telephone network communication facility. Using the wireless communication device 2, the computer 1 can establish a wireless data communication link 3 to a mobile telephone network 5 via a base station 4. The mobile telephone network 5 can connect to a remote computer (or server) 6 via an Internet link 7.

In-use, a user generates and/or modifies data on the computer l. When the user is finished generating or modifying the data, the user instructs the computer 1 to encrypt the data using conventional encryption software and then to establish a data communications link between the laptop computer 1 and the remote server 6. The computer 1 establishes the data communications link with the remote server 6 using the wireless communication device 2 to establish a wireless communication link 3 with the mobile telephone network 5 via the base station 4 to connect the laptop computer 1 to the remote server 6 via the Internet 7.

After the data communication link between the laptop computer 1 and the remote server 6 is established, the laptop computer 1 transfers the encrypted data to the remote server 6 to store the encrypted data on the remote server 6.

After the laptop computer 1 has received confirmation that the remote server 6 has correctly received the data, the laptop computer 1 terminates the data communication link to the server 6 by terminating the wireless communication link 3 to the mobile telephone network 5. After the data communication link has been terminated, the computer 1 then deletes the data on the computer and optimally deletes the encrypted data transmitted to the server 6. Deletion of the data can be performed using conventional deletion software.

Figure 2 is a flow chart illustrating the steps of the process described with reference to Figure 1 in more detail. Internet backup software 10 is carried on the laptop. When the user activates the software, the software automatically creates data sets (step 12), encrypts the data (step 14), compresses the data (step 16) and initiates the setting up of a connection to the Internet 7 for secure data transfer (step 18). The connection is established by any suitable proprietary software 20 that activates a PCMCIA card in the laptop (step 22), dials into a cellular network (step 24), and connects to an ISP (step 26) so that the laptop is connected to the Internet and to the secure data storage facility 6 connected to the Internet 7. After the laptop receives confirmation of the successful transfer of the data a Symantec wipe is performed on the laptop (step 28) that wipes data on the laptop to Department of Defense standards.

As an alternative to establishing a wireless communication link 3, the laptop computer 1 may establish the data communication link using a modem and a conventional landline or a computer network to which the computer 1 is connected and which is also connected to the Internet 7.

Figure 3 is a schematic illustration of a system embodying the present invention in which the laptop connects to a secure private network 30 via the Internet 7. Access to the private network is obtained via a 1-800 number ID and password. The private network 30 is connected to the secure data storage centre 6. It is also connected to the Internet via a firewall 38.

The invention has the advantage that by storing the data generated or modified on the computer 1 on the remote server 6, data can be retrieved from the server 6 without requiring the computer 1. This is an advantage if, for example, the computer 1is lost or stolen. In addition, the advantage of erasing the data, which is transmitted to the remote server 6, from the computer 1, is that if the computer 1 is lost or stolen, the risk of a recipient of the lost or stolen computer obtaining unauthorized access to the data is reduced.

Furthermore, encrypting the data prior to transmitting the data to the remote server also ensures that the data is stored in the remote server in an encrypted state and reduces the risk of unauthorized access to the data on the remote server or unauthorized access to the data while it is being transmitted to the remote server 6.

While the invention has been described with reference to specific embodiments, modifications and variations of the invention may be constructed without departing from the scope of the invention, which is defined in the following claims.